TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale No. PCT/FR 03/50202	Date du dépôt international *(jour/mois/année)* 22.12.2003	Date de priorité *(jour/mois/année)* 24.12.2002
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04N7/167, H04L9/08, H04N7/16		
Déposant VIACCESS		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 6 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des instructions administratives du PCT).

   Ces annexes comprennent 5 feuilles.

3. Le présent rapport contient des indications et les pages correspondantes relatives aux points suivants :

I	☒	Base de l'opinion
II	☐	Priorité
III	☐	Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
IV	☐	Absence d'unité de l'invention
V	☒	Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
VI	☐	Certains documents cités
VII	☐	Irrégularités dans la demande internationale
VIII	☐	Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
20.07.2004	20.12.2004
Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international Office européen des brevets - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Fonctionnaire autorisé Post, K N° de téléphone +31 70 340-2377

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR 03/50202

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale *(les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17))* :

Description, Pages

1-12 telles qu'initialement déposées

Revendications, No.

1-19 reçue(s) le 26.10.2004 avec lettre du 22.10.2004

Dessins, Feuilles

1/6-6/6 telles qu'initialement déposées

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

   Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: ,qui est:

   ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).

   ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).

   ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés**divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

   ☐ contenu dans la demande internationale, sous forme écrite.

   ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.

   ☐ remis ultérieurement à l'administration, sous forme écrite.

   ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

   ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

   ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

   ☐ de la description, pages :

   ☐ des revendications, nos :

   ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

   (Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui:	Revendications	1-19
	Non:	Revendications	
Activité inventive	Oui:	Revendications	
	Non:	Revendications	1-19
Possibilité d'application industrielle	Oui:	Revendications	1-19
	Non:	Revendications	

2. Citations et explications

   voir feuille séparée

Concernant le point V

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Il est fait référence aux documents suivants:

D1: EP-A-0 984 630 (MINDPORT BV) 8 mars 2000 (2000-03-08)
D2: US 2001/053221 A1 (TAKEDA TSUNEHARU) 20 décembre 2001 (2001-12-20)

2. La présente demande ne remplit pas les conditions énoncées dans l'article 33(1) PCT, l'objet des **revendications 1-19** n'impliquant pas une activité inventive telle que définie par l'article 33(3) PCT.

2.1 Le document D1, qui est considéré comme étant l'état de la technique le plus proche, décrit (cf. surtout col. 2, lignes 8-29 et les autres passages cités ci-dessous):

procédé de sécurisation de données embrouillées fournies à une pluralité de terminaux récepteurs ("decrypting a message, for example the encrypted payload in a pay TV transport stream"), chacun desdits terminaux étant muni d'une pluralité de modules de désembrouillage Mj, j=1,2, ("first and second decryption devices") ayant chacun une capacité de traitement et un niveau de sécurité spécifique (le premier module est un "smart card" ayant "very high security" et le deuxième peut être un "PC or microprocessor"),
lesdites données étant préalablement subdivisées en un nombre entier de familles Fj comportant chacune un nombre entier de blocs Bi (le message est divisé en blocs dont certains sont envoyés au premier module et d'autres au deuxième, cf. col. 2, lignes 17-21 et aussi col. 1, lignes 46-51),
chaque bloc B1 envoyé au premier module étant embrouillé par une clé K1 ("secret key", col. 2, ligne 13),
procédé caractérisé en ce que lesdits bloc Bi sont préalablement organisés en fonction des vitesse respectives de traitement des modules de désembrouillage Mj. (Les blocs dans D1 sont organisés tels que le premier bloc d'un groupe de x blocs soit envoyé au premier module, qui a une vitesse de traitement plus lente que le deuxième module, voir encore col. 1, lignes 46-51, col. 2, lignes 17-21 et la revendication 6.)

Par conséquent, l'objet de la **revendication 1** de la demande diffère de ce procédé connu seulement en ce que les blocs envoyés au deuxième module (le "PC") sont embrouillés par une clé K2 et en ce que les clés Kj sont définies en fonction de la capacité de traitement et du degré de sécurité des modules de déchiffrement respectifs Mj (j=1,2).
Dans le document D1 on applique un algorithme plus élaboré ("error-propagating block chaining method", cf. col. 2, lignes 26-27) pour sécuriser davantage ce deuxième module et il serait très évident pour la personne du métier d'utiliser la dite méthode d'embrouiller les blocs envoyés aux modules Mj avec des clés Kj différentes pour simplifier la méthode si cet effet supplémentaire n'était pas désiré. Pour cela elle choisirait de manière évidente les clés Kj en fonction de la capacité de traitement et du degré de sécurité des modules de déchiffrement Mj afin d'utiliser au maximum leurs puissances de calcul respectives.

2.2 La **revendication indépendante 13** diffère du procédé connu en plus en ce que un paramètre d'identification pj affecté à chaque famille Fj soit explicitement mentionné. Comme les blocs envoyés au premier module dans le procédé de D1 ne sont pas fixes (cf. col. 1, lignes 49-51: "the number of intermediate blocks is not fixed but may vary as desired"), une sorte d'identification de famille doit être utilisée implicitement.
Cette caractéristique a toutefois déjà été employée dans le même but dans un procédé analogue dans le document D2 (voir l'abrégé) : D2 décrit un procédé de sécurisation de données embrouillées fournies à une pluralité de terminaux récepteurs avec un seule module de désembrouillage. Dans ce procédé les données sont aussi subdivisées en familles Fj *et explicitement* identifiées par des paramètres pj ("ciphering attribute") et chiffrées selon ces paramètres, qui aussi identifient les clés à utiliser (voir page 2, paragraphe [42]).
Il est alors évident pour la personne du métier d'appliquer les caractéristiques additionnelles dans le procédé suivant le document D1 et d'obtenir ainsi l'objet de la revendication 13.

2.3 Il est également évident d'utiliser le dit procédé pour sécuriser différents services comme ceux mentionnés dans les **revendications 17-19** qui par conséquent ne sont pas inventives non plus.

2.4 Les **revendications dépendantes 2-12 et 14-16** ne contiennent aucune caractéristique qui, en combinaison avec celles de l'une quelconque des revendications à laquelle elles se réfèrent, définisse un objet qui satisfasse aux exigences du PCT en ce qui concerne l'activité inventive, parce que toutes les caractéristiques additionnelles

sont déjà décrites dans les documents D1 ou D2 ou bien triviales.

REVENDICATIONS

1. Procédé de sécurisation de données embrouillées fournies à une pluralité de terminaux récepteurs, chacun desdits terminaux étant muni d'une pluralité de modules de désembrouillage Mj (j=1...M) ayant chacun une capacité de traitement et un niveau de sécurité spécifique, lesdites données étant préalablement subdivisées en un nombre entier de familles Fj (j=1...M) comportant chacune un nombre entier de blocs Bi (i=1...N), procédé caractérisé en ce que :

- à l'émission, chaque bloc Bi (i=1...N) d'une famille Fj est embrouillé par une clé Kj (j=1...M) associée à la famille Fj, définie en fonction de la capacité de traitement et du degré de sécurité des modules de déchiffrement respectifs Mj (j=1...M), et
- à la réception, chaque bloc Bi (i=1...N) d'une famille Fj est désembrouillé au moyen de la clé Kj (j=1...M) associée à la famille Fj.

2. Procédé selon la revendication 1, caractérisé en ce que les modules Mj (j=1...M) sont des éléments périphériques différents associés audit terminal récepteur.

3. Procédé selon la revendication 2, caractérisé en ce que les modules de désembrouillage Mj (j=1...M) comportent des algorithmes Aj (j=1...M) différents.

4. Procédé selon la revendication 2, caractérisé en ce que les module de désembrouillage Mj (j=1...M) comportent des algorithmes Aj (j=1...M) identiques.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que les données à distribuer se présentent sous forme d'un fichier préalablement mémorisé.

6. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que les données à sécuriser se présentent sous forme d'un flux diffusé ou téléchargé et traité en temps réel par le terminal.

7. Procédé selon les revendications 5 ou 6, caractérisé en ce que la durée d'utilisation du flux est divisée en crypto-périodes correspondant chacune à une clé de désembrouillage, et en ce qu'avant chaque début de crypto-période un message est inséré dans le flux afin de prévenir le module de désembrouillage Mj du changement de crypto-période.

8. Procédé selon la revendication 7, caractérisé en ce que ledit message comporte l'ensemble des informations nécessaires pour désembrouiller le flux utilisé pendant la crypto-période suivante.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que lesdites données représentent des programmes audio et/ou vidéo protégés par un système DRM.

10. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que lesdites données représentent

des images de synthèse ou des dessins animés.

11. Système de sécurisation de données embrouillées fournies à au moins un terminal récepteur, caractérisé en ce qu'il comporte :

- une plate-forme d'embrouillage comprenant :
  - des moyens pour subdiviser lesdites données en m familles distinctes de N blocs Bi (i=1...N),
  - des moyens pour affecter à chaque famille Fj un paramètre spécifique d'identification pj (j=1...M) associé à au moins un module de désembrouillage Mj ayant une capacité de traitement et un niveau de sécurité spécifiques,
  - des moyens pour embrouiller chaque bloc Bi par une clé Kj (j=1...M) en relation biunivoque avec le paramètre pj,
- et une plate-forme de désembrouillage comportant des moyens pour identifier la famille de chaque bloc Bi de manière à désembrouiller chaque bloc Bi d'une famille de type pj par le module Mj correspondant audit paramètre pj.

12. Système selon la revendication 11, caractérisé en ce que les modules de désembrouillages distincts Mj (j=1...M) sont des périphériques distincts associés au terminal récepteur.

13. Plate-forme d'embrouillage d'un flux de données, caractérisée en ce qu'elle comporte :

- des moyens pour subdiviser ledit flux en m familles distinctes Fj (j=1...M) de N blocs Bi (i=1...N),

- des moyens pour affecter à chaque famille Fj (j=1...M) un paramètre spécifique d'identification pj (j=1...M) associé à au moins un module de désembrouillage Mj ayant une capacité de traitement et un niveau de sécurité spécifiques,

- des moyens pour définir pour chaque module Mj (j=1...M) une clé Kj (j=1...M) en fonction de la capacité de traitement et du degré de sécurité dudit Mj (j=1...M),

- des moyens pour embrouiller chaque bloc Bi appartenant à une famille Fj (j=1...M) par une clé Kj (j=1...M) en relation biunivoque avec le paramètre pj.

14. Plate-forme de désembrouillage d'un flux de données embrouillé par la plate-forme de la revendication 13, caractérisée en ce qu'elle comporte des moyens pour identifier la famille de chaque bloc Bi de manière à désembrouiller chaque bloc Bi d'une famille de type pj par le module Mj correspondant audit paramètre pj.

15. Plate-forme de désembrouillage selon la revendication 14, caractérisée en ce qu'elle comporte une pluralité de modules de désembrouillage distincts Mj (i=1...M) identifiés chacun par le paramètre spécifique d'identification pj.

16. Plate-forme de désembrouillage selon la revendication 15, caractérisée en ce que le terminal récepteur est un PDA et en ce que l'un desdits modules de désembrouillage Mj (i=1...M) est intégré au PDA et au moins deuxième module est une carte à puce de type SIM

connectée audit PDA.

17. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser un service de vidéo à la demande (VOD).

18. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser un service de Musique à la demande (MOD).

19. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser l'accès à un service diffusion de livre électronique en ligne ou téléchargé à partir d'un support amovible.